REMARKS

The following remarks are made in response to the Office Action mailed November 26, 2010. Claims 7-9, 31, 33, and 34 have been previously cancelled. Claims 1-6, 10-30, 32, and 35-58 were rejected. With this Response, no claims have been amended. Claims 1-6, 10-30, 32, and 35-58 remain pending in the application and are presented for reconsideration and allowance.

Claim Rejections under 35 U.S.C. § 102

The Examiner rejected claims 1-6, 10, 12, 17-23, 25-30, 32, 36, 41-47, and 49-58 under 35 U.S.C. § 102(e) as being anticipated by Narayanan, U.S. Patent Application Publication No. 2005/0021946 ("Narayanan").

Applicants submit that Narayanan fails to teach or suggest the features recited by independent claim 1 including "**providing, by a first node, a component value A1; providing, by an adjacent node, a component value B1 as a challenge to the first node; performing, by the first node, a handshake process with the adjacent node to determine membership in a secure group; wherein the handshake process comprises requiring each of the first node and the adjacent node to calculate identical values by applying the component values A1 and B1, and a key value associated with the secure group, to a one way function f(x).**"

Narayanan discloses a method and communication system that includes a plurality of nodes communicating in a shared network segment. A node (i.e., a router) that boots up or starts a protocol application sends a multicast start message on the specific multicast channel. Another node receiving this start message validates the authenticity of the start message and may send a response message. (Para. [0015]). If a node does not receive any message on the "Start-up" channel, then it sends a "jump-start" message signed by the node's private key. (Para. [0039]).

The jump-start packet for a router R1 may include the fields: Source IP Address, Destination IP Address, Random Value (or Time Stamp), and Digital Signature (DS1). (Para. [0044] – [0048]). The router R1 generates the digital signature DS1 as follows: DS1 = Enc(Source Address, Random Value, Private Key of Router 1). (Para. [0051] – [0052]). A

router R2 listens on the start-up channel, receives the jump-start packet, and verifies the digital signature DS1 thereof by forming a digital signature DS2 as follows: DS2 = Enc(Source Address, Random Value, Public Key of Router 1). (Para. [0053] – [0054]). Router R2 compares the DS1 and DS2 and decides that router R1 is valid and accepted by router R2 when DS1 = DS2. (Para. [0055]). When DS1 is not equal to DS2, router R2 decides that router R1 is not valid and does not accept router R1. (Para. [0056]).

The Examiner submits that digital signature DS1 and digital signature DS2 of Narayanan disclose the *component value A1* and the *component value B1*, respectively, as recited by claim 1. (Office Action, page 3). The Examiner further submits that Narayanan discloses the *handshake process* recited by claim 1 in that Narayanan discloses that router R2 verifies that router R1's transmittal of DS1 is equal to router R2's DS2. (Office Action, page 3).

Digital signature DS1 and digital signature DS2 of Narayanan do not provide a *component value A1* and a *component value B1* for a *one way function f(x)*. In contrast, digital signatures DS1 and DS2 are the result of the calculations: DS1 = Enc(Source Address, Random Value, Private Key of Router 1) and DS2 = Enc(Source Address, Random Value, Public Key of Router 1). Digital signature DS1 is not used to calculate digital signature DS2, and digital signature DS2 is not used to calculate digital signature DS1. Therefore, Narayanan fails to disclose a *component value A1* of a first node or a *component value B1* of an adjacent node that are applied to a one way function f(x).

In addition, Narayanan fails to disclose *a key value associated with the secure group* and applying the key value to the one way function f(x). Router R1 and router R2 of Narayanan do not share a common key value. In contrast, router R1 has a private key of router R1 and router R2 has the public key of router R1. Router R2 does not know the private key of router R1. The calculations DS1 = Enc(Source Address, Random Value, Private Key of Router 1) and DS2 = Enc(Source Address, Random Value, Public Key of Router 1) use different key values (i.e., the private and public key of router R1). The calculations do not use a common key value associated with the secure group as recited by claim 1.

The Examiner submits that the *identical values* recited by claim 1 are disclosed by digital signatures DS1 and DS2 of Narayanan. (Office Action, page 3). The digital signatures DS1 and DS2 cannot be both the identical values and the component values A1 and B1 recited by claim 1 since the component values A1 and B1 are applied to the one way function f(x) to calculate the identical values. Narayanan fails to disclose that router R1 and router R2 calculate identical values by applying the component values A1 and B1, and a key value associated with the secure group to a one way function.

In view of the above, Applicants submit that the above rejection of independent claim 1 under 35 U.S.C. § 102(e) should be withdrawn. Dependent claims 2-6, 10, 12, 17-23, 51, and 52 further define patentably distinct independent claim 1. Accordingly, for at least the reasons remarked above with reference to independent claim 1, Applicants believe that these dependent claims are also allowable over the cited reference.

In addition, Applicants submit that Narayanan also fails to teach or suggest the further features recited by dependent claim 10 including **"wherein the one way function f(x) is a secure hash function."**

The Examiner submits that paragraph [0083] of Narayanan teaches this feature. (Office Action, page 5). Narayanan discloses that when the designated router DR is the only available node in the segment, the DR uses its public/private key pair and determines a random session key. This session key can be generated as follows: Key=Hash(Random Number, private Key, Public Key, Time Stamp). (Para. [0083]).

The generation of a session key for a router with no other routers in the segment is not at all related to the handshake process between two routers. The Examiner submitted that the calculation of digital signatures DS1 and DS2 of Narayanan disclosed the one way function f(x) recited by claim 1, from which claim 10 depends. The session key mentioned in paragraph [0083] of Narayanan is not digital signature DS1 or DS2. The session key mentioned in paragraph [0083] of Narayanan is not used in any handshaking process since the mentioned session key is used when there is only one node.

Further, the Examiner summarily rejected dependent claims 17-23 based on paragraphs [0066], [0093] – [0094], and [0085] – [0087] of Narayanan. (Office Action, page 5). Narayanan discloses that a session key update packet may include a time stamp. (Para.

[0066]). Narayanan also discloses that short-term keys are derived using a long-term key. The life-time of a short term key is valid only for that session. In addition, the short term keys are also refreshed periodically at regular intervals. (Para. [0093] – [0094]). Narayanan further discloses that when other nodes join or leave a group the group-keys have to be changed and new keys have to be distributed. (Para. [0085] – [0087]).

Narayanan, including the Examiner cited portions, fails to teach or suggest the further features recited by dependent claim 17 including "**wherein the action of determining the age of the secure information comprises: checking a sequence number of the secure information to determine the age of the secure information;**" the features recited by dependent claim 18 including "**wherein the action of determining the age of the secure information comprises: checking a date of modification of the secure information to determine the age of the secure information;**" the features recited by dependent claim 19 including "**wherein the action of determining the age of the secure information comprises: checking an elapsed time since a previous modification of the secure information to determine the age of the secure information;**" the features recited by dependent claim 20 including "**resolving an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value;**" the features recited by dependent claim 21 including "**increasing a security of the secure group by widening the key value which is known by each node in the secure group;**" the features recited by dependent claim 22 including "**decreasing an amount of time between symmetric key regeneration (TK) to increase the security of the secure group;**" and the features recited by dependent claim 23 including "**allowing for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes.**"

While Narayanan discloses a time stamp, Narayanan does not disclose that the time stamp is used in any of the above recited features of claims 17-23. The Examiner has failed to specifically point out how Narayanan discloses each of the features recited by claims 17-23.

In view of the above, Applicants submit that the above rejection of dependent claims 2-6, 10, 12, 17-23, 51, and 52 under 35 U.S.C. § 102(e) should be withdrawn. Allowance of claims 1-6, 10, 12, 17-23, 51, and 52 is respectfully requested.

For similar reasons as remarked above with reference to independent claim 1, Applicants submit the Narayanan also fails to teach or suggest the features recited by independent claim 25 including "**wherein the handshake process comprises requiring each of the node and the adjacent node to calculate identical values by applying a component value A1 provided by the node, a component value B1 provided by the adjacent node, and a key value associated with the secure group, to a one way function f(x);**" and the features recited by independent claims 49 and 50 including "**wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to calculate identical values by applying a component value A1 provided by the first node, a component value B1 provided by the adjacent node, and the key value associated with the secure group, to a one way function f(x).**"

In view of the above, Applicants submit that the above rejection of independent claims 25, 49, and 50 under 35 U.S.C. § 102(e) should be withdrawn. Dependent claims 26-30, 32, 36, 41-47, and 53-58 further define patentably distinct independent claim 25, 49, or 50. Accordingly, for at least the reasons remarked above with reference to independent claims 25, 49, and 50, Applicants believe that these dependent claims are also allowable over the cited reference.

In addition, for similar reasons as remarked above with reference to dependent claim 10, Applicants submit the Narayanan also fails to teach or suggest the further features recited by dependent claim 32 including "**wherein the one way function f(x) is a secure hash function.**"

Further, for similar reasons as remarked above with reference to dependent claims 17-23, Applicants submit the Narayanan also fails to teach or suggest the further features recited by dependent claim 41 including "**wherein the node is configured to check a sequence number of the secure information to determine the age of the secure information;**" the features recited by dependent claim 42 including "**wherein the node is configured to check**

a date of modification of the secure information to determine the age of the secure information;" the features recited by dependent claim 43 including "**wherein the node is configured to check an elapsed time since a previous modification of the secure information to determine the age of the secure information**;" the features recited by dependent claim 44 including "**wherein the node is configured to resolve an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value**;" the features recited by dependent claim 45 including "**wherein the node is configured to increase a security of the secure group by widening the key value which is known by each node in the secure group**;" the features recited by dependent claim 46 including "**wherein the node is configured to decrease an amount of time between symmetric key regeneration (TK) to increase the security of the secure group**;" and the features recited by dependent claim 47 including "**wherein the node is configured to allow for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes**."

While Narayanan discloses a time stamp, Narayanan does not disclose that the time stamp is used in any of the above recited features of claims 41-47. The Examiner has failed to specifically point out how Narayanan discloses each of the features recited by claims 41-47.

In view of the above, Applicants submit that the above rejection of dependent claims 26-30, 32, 36, 41-47, and 53-58 under 35 U.S.C. § 102(e) should be withdrawn. Allowance of claims 25-30, 32, 36, 41-47, 49, 50, and 53-58 is respectfully requested.

Claim Rejections under 35 U.S.C. § 103

The Examiner rejected claims 11, 13, 16, 35, 37, and 40 under 35 U.S.C. § 103(a) as being unpatentable over Narayanan in view of Traversat et al., U.S. Patent Application Publication No. 2002/0152299 ("Traversat").

Dependent claims 11, 13, 16, 35, 37, and 40 further define patentably distinct independent claim 1 or 25. Accordingly, for at least the reasons remarked above with

reference to independent claims 1 and 25, Applicants believe that these dependent claims are also allowable over the cited references. Allowance of claims 11, 13, 16, 35, 37, and 40 is respectfully requested.

The Examiner rejected claims 14, 15, 38, and 39 under 35 U.S.C. § 103(a) as being unpatentable over Narayanan in view of Traversat and further in view of Mowers et al., U.S. Patent No. 7,644,275 ("Mowers").

Dependent claims 14, 15, 38, and 39 further define patentably distinct independent claim 1 or 25. Accordingly, for at least the reasons remarked above with reference to independent claims 1 and 25, Applicants believe that these dependent claims are also allowable over the cited references. Allowance of claims 14, 15, 38, and 39 is respectfully requested.

The Examiner rejected claims 24 and 48 under 35 U.S.C. § 103(a) as being unpatentable over Narayanan in view of Dondeti et al., U.S. Patent No. 6,240,188 ("Dondeti").

Dependent claims 24 and 48 further define patentably distinct independent claim 1 or 25. Accordingly, for at least the reasons remarked above with reference to independent claims 1 and 25, Applicants believe that these dependent claims are also allowable over the cited references. Allowance of claims 24 and 48 is respectfully requested.

CONCLUSION

In view of the above, Applicants respectfully submit that pending claims 1-6, 10-30, 32, and 35-58 are in form for allowance and are not taught or suggested by the cited references. Therefore, reconsideration and withdrawal of the rejections and allowance of claims 1-6, 10-30, 32, and 35-58 is respectfully requested.

The Examiner is invited to contact the Applicants' representative at the below-listed telephone numbers to facilitate prosecution of this application.

Any inquiry regarding this Response should be directed to Mark A. Peterson at Telephone No. (612) 573-0120, Facsimile No. (612) 573-2005.

Respectfully submitted,

Michael Roeder et al.

By their attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2000
Facsimile: (612) 573-2005

Date: February 2, 2011
MAP:cjs

/Mark A. Peterson/
Mark A. Peterson
Reg. No. 50,485